



Marine Corps Intrusion Detection and Analysis Section (MIDAS)

Overview of Operations and
Capabilities
2000



MIDAS MISSION

The MIDAS provides security centric network support at the Tactical, Operational and strategic levels to the operational war fighter as well as Posts, Bases and Stations that support the Marine Corps War Fighter

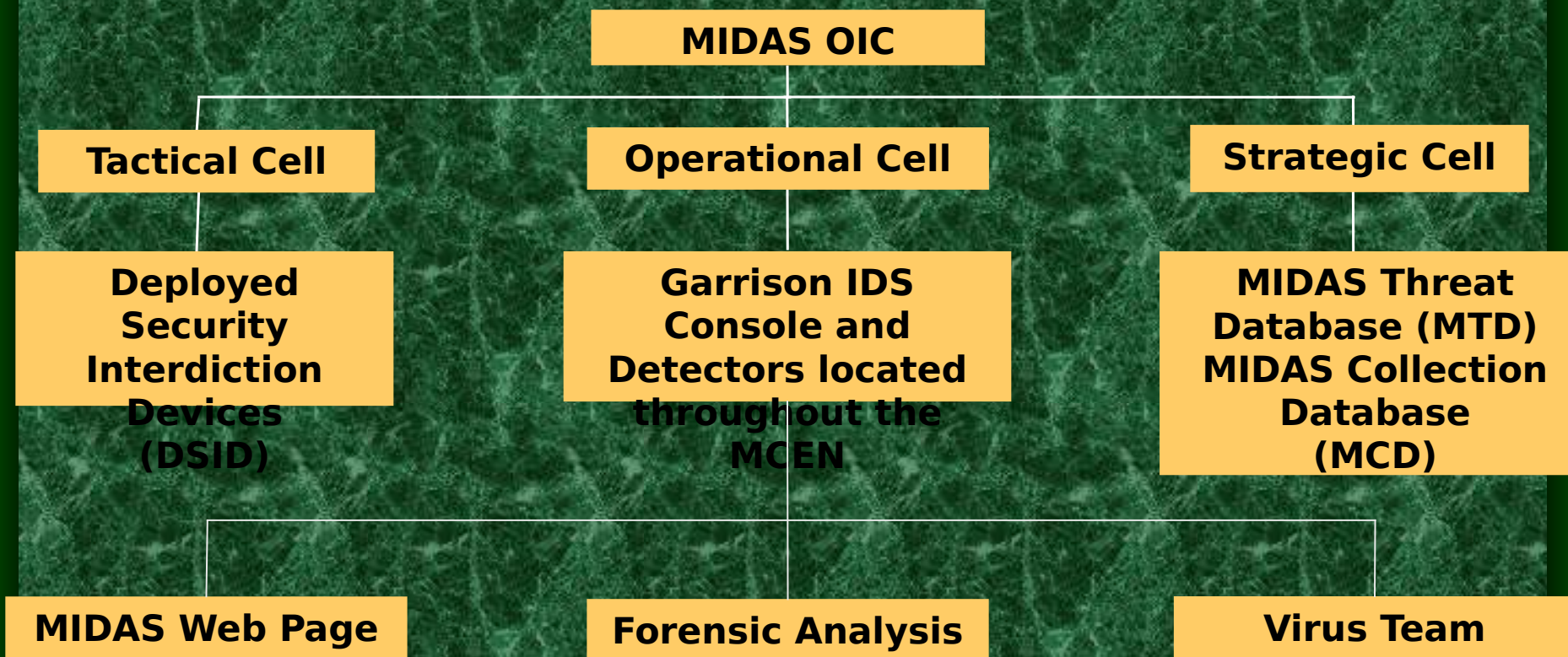


Mission Accomplished Through:

- Intrusion Detection
- Incident Handling
- Threat Analysis
- Virus Team
- Deployed Support
- Vulnerability Assessment



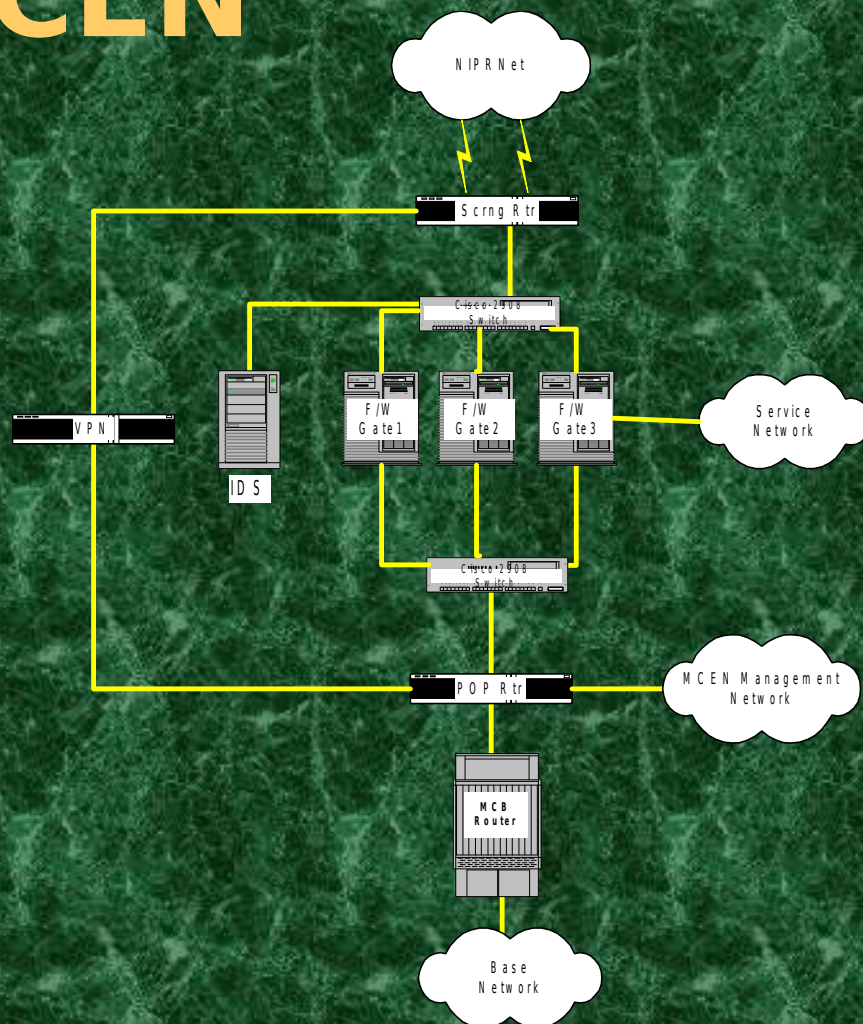
MIDAS Immediate Chain of Command





Topology of IDS in the MCEN

- Defense-in-Depth Strategy
- That which is not strictly permitted is denied
- IDS Technology





Tools Used to Aid CND

- Intrusion Detection System (RealSecure – COTS)
- Data Aggregation Tools
 - Routers
 - Firewalls
 - IDS
- MIDAS Collection Database (MCD)
- MIDAS Threat Database (MTD)



Intrusion Detection:

- Systems that collect information from a variety of systems and network resources, then analyze the information for signs of intrusion and misuse in near real-time.



Benefits of Intrusion Detection

- Improving the integrity of the information security infrastructure
- Improve system monitoring
- Tracing user activity from point of entry to point of exit or impact
- Recognizing and reporting alterations to data files



Benefits of Intrusion-Detection cont:

- Spotting errors of system configuration and sometimes correcting them
- Recognizing specific types of attacks and alerting appropriate staff for defensive responses
- keeping system management personnel up to date on recent corrections to programs



RealSecure Components

- **Detectors -**
 - Network Engine for network-based intrusion detection
 - System Agent for host-based intrusion detection
- **Management Console -** Provides:
 - Central Real-time alarm management
 - Central data management
 - Central detector configuration



Management Console

- Collects databases from active detectors into a single data store:
 - For export to an enterprise database system
 - To generate reports



Network Detectors

- Captures all packets from a local network segment
- Examines each packet for signs of:
 - Network abuse
 - Malicious intent
 - Suspicious activity



Network Detectors cont.



- Users can customize by:
 - Defining connection events
 - Specifying a response for every single event
 - Fine-tuning existing signatures
 - Establish traffic masking filters



RealSecure Demo





Console Main Screen

RealSecure

File View Window Help

Ready

Activity Tree

View

- Active Events (34 events)
 - SYNFlood (16 events)
 - 0.0.0.0 (16 events)
 - IPDuplicate (4 events)
 - IPProtocolViolation (1 event)
 - Detector_Info (12 events)

High Priority

Detector	Event	From	To	Info	Date
Cherry_Point	IPDuplicate	192.156.73.33	192.156.73.46	MAC1 - 00:E0:1...	Sat Jun 03 18:01:16 2000
Cherry_Point	SYNFlood	0.0.0.0	209.249.123.182	SPOOFEDSRC	Sat Jun 03 18:01:20 2000
Cherry_Point	SYNFlood	0.0.0.0	216.200.247.134	SPOOFEDSRC	Sat Jun 03 18:02:17 2000
Cherry_Point	SYNFlood	0.0.0.0	209.249.123.210	SPOOFEDSRC	Sat Jun 03 18:02:52 2000
Cherry_Point	IPDuplicate	192.156.73.33	192.156.73.34	MAC1 - 00:E0:1...	Sat Jun 03 18:06:43 2000
Cherry_Point	IPDuplicate	192.156.73.33	192.156.73.35	MAC1 - 00:E0:1...	Sat Jun 03 18:11:22 2000
Cherry_Point	IPDuplicate	192.156.73.33	192.156.73.46	MAC1 - 00:E0:1...	Sat Jun 03 18:11:22 2000
Cherry_Point	IPDuplicate	192.156.73.33	192.156.73.34	MAC1 - 00:E0:1...	Sat Jun 03 18:16:43 2000
Cherry_Point	IPDuplicate	192.156.73.33	192.156.73.43	MAC1 - 00:E0:1...	Sat Jun 03 18:18:35 2000

Medium Priority

Detector	Event	From	To	Info	Date
Cherry_Point	IPProtocolViolat...	208.11.184.123	158.245.80.141	REASON - Unu...	Sat Jun 03 04:17:35
Cherry_Point	IPProtocolViolat...	208.11.184.123	158.245.80.141	REASON - Unu...	Sat Jun 03 04:18:05

Low Priority

Detector	Event	From	To	Info	Date
MARFORTLA...	Detector_Info	192.156.69.46	192.156.69.46	Message - Eve...	Sat Jun 03 04:50:53 2000
MARFORTLA...	Detector_Info	192.156.69.46	192.156.69.46	Message - Eve...	Sat Jun 03 06:51:15 2000
MARFORTLA...	Detector_Info	192.156.69.46	192.156.69.46	Message - Eve...	Sat Jun 03 08:51:35 2000
MARFORTLA...	Detector_Info	192.156.69.46	192.156.69.46	Message - Eve...	Sat Jun 03 12:38:41 2000
MARFORTLA...	Detector_Info	192.156.69.46	192.156.69.46	Message - Eve...	Sat Jun 03 14:38:55 2000
MARFORTLA...	Detector_Info	192.156.69.46	192.156.69.46	Message - Eve...	Sat Jun 03 17:50:16 2000

Source Destination Events

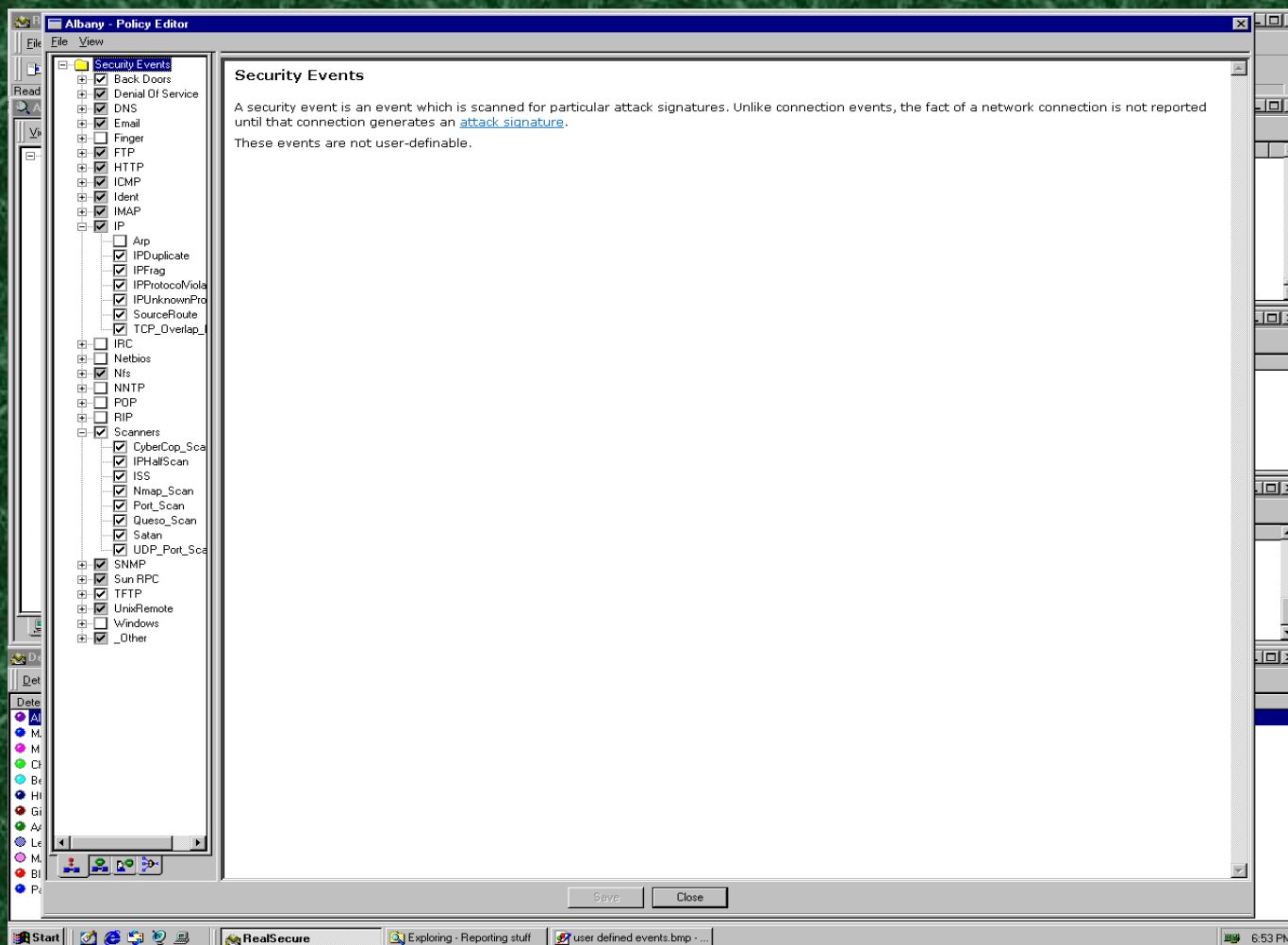
Detectors

Detector	Location	Policy	Detector Status	Event Channel Status	Detector DB Progress
Albany	192.156.74.46	EastCoast_Phuto : PLUTO - Wed May 31 07:45:18 2000	Active	Established	DB Sync Done.
MARFORTLANT	192.156.69.46	EastCoast_Phuto : PLUTO - Wed May 31 07:43:01 2000	Active	Established	DB Sync Done.
MCI_8Hl	192.156.46.46	EastCoast_Phuto : PLUTO - Wed May 31 07:44:17 2000	Active	Established	DB Sync Done.
Cherry_Point	192.156.73.46	EastCoast_Phuto : PLUTO - Wed May 31 07:46:29 2000	Active	Established	DB Sync Done.
Beaufort	192.156.70.46	EastCoast_Phuto : PLUTO - Wed May 31 07:47:41 2000	Active	Established	DB Sync Done.
HQMC	192.156.13.46	EastCoast_Phuto : PLUTO - Wed May 31 07:49:41 2000	Active	Established	DB Sync Done.
Gilmo	192.156.28.46	EastCoast_Phuto : PLUTO - Wed May 31 07:58:56 2000	Active	Established	DB Sync Done.
AAAV	192.156.27.46	EastCoast_Phuto : PLUTO - Wed May 31 07:52:02 2000	Active	Established	DB Sync Done.
Lejeune	192.156.37.46	EastCoast_Phuto : PLUTO - Wed May 31 07:53:30 2000	Active	Established	DB Sync Done.
MARFORRES	192.156.26.46	EastCoast_Phuto : PLUTO - Wed May 31 07:55:52 2000	Active	Established	DB Sync Done.
Blount_Island	192.156.14.46	EastCoast_Phuto : PLUTO - Wed May 31 07:56:50 2000	Active	Established	DB Sync Done.
Paris_Island	192.156.36.46	EastCoast_Phuto : PLUTO - Wed May 31 07:57:51 2000	Active	Established	DB Sync Done.

Start RealSecure 6:42 PM



Policy Editor





Connection Events

MARFORTLANT - Policy Editor

File View

☒ Connection Events

Connection Events

Add Remove

	Enabled	Event	Priority	Response	Src Address	Dest Address	Protocol	Src Port/Type	Dest Port/Code
1	<input checked="" type="checkbox"/>	CARTER-1	High		194.226.177.0/24	Any	tcp	Any	Any
2	<input checked="" type="checkbox"/>	CARTER-2	High		Any	194.226.177.0/24	tcp	Any	Any
3	<input checked="" type="checkbox"/>	ANS-IN	High		207.24.114.0/24	Any	tcp	Any	Any
4	<input checked="" type="checkbox"/>	ANS-OUT	High		Any	207.24.114.0/24	tcp	Any	Any
5	<input checked="" type="checkbox"/>	UK-ISS Scan in	High		128.40.234.0/24	Any	icmp	Echo Reply	Network
6	<input checked="" type="checkbox"/>	UK-ISS Scan out	High		Any	128.40.234.0/24	icmp	Echo Reply	Network
7	<input checked="" type="checkbox"/>	NOC-SSH-PORT	High		Any	192.156.0.0/16	tcp	Any	ssh

Connection Events

A user-definable notification of an open connection to or from a particular address. Unlike other attacks, the console is notified when network activity is monitored at a designated port, regardless of the type of activity. For example, you can define a connection event to alert the console whenever an FTP connection is made, but the connection is not monitored for any particular attack signatures.

Note: The connections are always registered against the user-supplied destination port, so to monitor an FTP connection, you must use the FTP port. One entry per connection is sufficient for traffic in each direction.

Save Close



User Defined Events

MARFORTLANT - Policy Editor

File View

☒ User Defined Event

User Defined Events

Add Remove

	Enabled	Event	Priority	Response	Context	String
1	<input checked="" type="checkbox"/>	MSADCS_Exploit	High		URL_Data	Vmsadc\Vmsadcs*.dll

User-Defined Events

It is possible to construct custom rules for monitoring system activities. These rules can monitor any of the primary data sources for specific messages. These data sources are the NT Event Logs for monitoring activity on an NT host, UNIX Syslog messages for monitoring a remote UNIX host, and Suspicious Port events for detecting the suspicious use of unused ports.

Save Close



Filters

MARFORTLANT - Policy Editor

File View

☒ Filters

User-Specified Filters

	Enabled	Filter	Src Address	Dest Address	Protocol	Src Port/Type	Dest Port/Code
1	<input checked="" type="checkbox"/>	SSH-Filter	192.156.75.55/32	Any	tcp	SSH	Any
2	<input checked="" type="checkbox"/>	noc-ssh	192.156.0.0/16	192.156.0.0/16	tcp	Any	ssh

Filters

Filters allow RealSecure to ignore certain types of network traffic. You can use filters to prevent parts of your network from being monitored.



Event Inspector

Event Inspector [?] [X]

Event	Date
IPDuplicate	Sat Jun 03 18:31:30 200
IPDuplicate	Sat Jun 03 18:11:22 200
IPDuplicate	Sat Jun 03 18:01:16 200
IPDuplicate	Sat Jun 03 17:51:09 200
IPDuplicate	Sat Jun 03 17:41:06 200
IPDuplicate	Sat Jun 03 17:20:40 200
IPDuplicate	Sat Jun 03 17:10:27 200
IPDuplicate	Sat Jun 03 17:00:12 200
IPDuplicate	Sat Jun 03 16:49:49 200
IPDuplicate	Sat Jun 03 16:29:39 200
IPDuplicate	Sat Jun 03 16:19:37 200
IPDuplicate	Sat Jun 03 15:59:02 200
IPDuplicate	Sat Jun 03 15:48:58 200
IPDuplicate	Sat Jun 03 15:38:09 200
IPDuplicate	Sat Jun 03 15:28:05 200
IPDuplicate	Sat Jun 03 15:07:48 200
IPDuplicate	Sat Jun 03 14:47:39 200
IPDuplicate	Sat Jun 03 14:37:13 200
IPDuplicate	Sat Jun 03 14:17:07 200
IPDuplicate	Sat Jun 03 14:06:48 200
IPDuplicate	Sat Jun 03 13:46:39 200
IPDuplicate	Sat Jun 03 13:25:39 200
IPDuplicate	Sat Jun 03 13:15:37 200
IPDuplicate	Sat Jun 03 12:55:28 200
IPDuplicate	Sat Jun 03 12:45:27 200

Event : IPDuplicate
Date: Sat Jun 03 18:31:30 2000
Source Addr: cpts1.cherrypoint.usmc.mil
Destination Addr: gate2.cherrypoint.usmc.mil
Detector Location: 192.156.73.46
☒ Resolve Addresses
Protocol: ARP

Info Type	Info Value
MAC1	00:E0:1E:8E:9E:D9
MAC2	00:E0:1E:8E:9E:E0

Actions Taken
Log To Database

Close Help



Event Name Report

d:\Program Files\MSS\RealSecure 3.2\Reports\eventname.rpt

31 of 31+ 100% Total:1755 100% 1755 of 157386

Preview

- eventname.rpt
 - IPDuplicate
 - IPHaltScan
 - IPProtocolV
 - IPUnknown
 - Nmap_Scan
 - RealSecure
 - SYNFlood

Event Name Report

Generated: 6/3/00 7:01:08PM

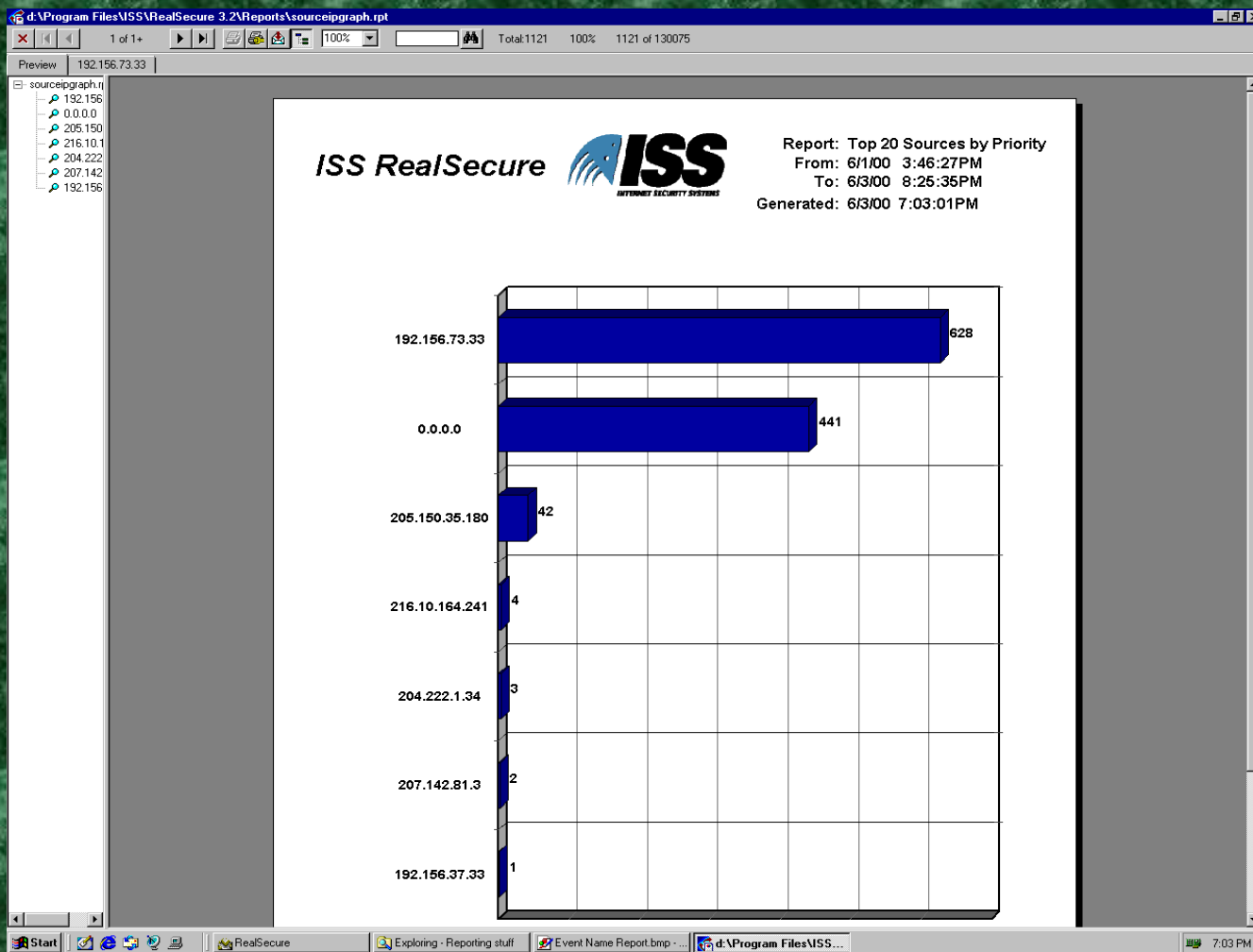
Event:	Priority	Date	From	To	Information
IPDuplicate					MAC2 00:E0:1E:8E:9E:E0
Event:					
IPHaltScan					
Priority	Date	From	To	Information	
High	6/1/00 5:30:54PM	205.150.35.180	158.245.250.75		
High	6/1/00 5:30:59PM	205.150.35.180	158.245.250.75		
High	6/1/00 5:31:07PM	205.150.35.180	158.245.250.75		
High	6/1/00 7:45:32PM	205.150.35.180	158.245.89.218		
High	6/1/00 7:45:43PM	205.150.35.180	158.245.89.218		
High	6/1/00 7:45:55PM	205.150.35.180	158.245.89.218		
High	6/2/00 1:10:26AM	205.150.35.180	205.101.172.20		
High	6/2/00 1:10:31AM	205.150.35.180	205.101.172.20		
High	6/2/00 1:10:35AM	205.150.35.180	205.101.172.20		
High	6/2/00 6:51:01AM	205.150.35.180	158.245.80.39		
High	6/2/00 6:51:06AM	205.150.35.180	158.245.80.39		
High	6/2/00 6:51:11AM	205.150.35.180	158.245.80.39		
High	6/2/00 1:38:33PM	205.150.35.180	158.245.134.161		
High	6/2/00 1:38:38PM	205.150.35.180	158.245.134.161		
High	6/2/00 1:38:42PM	205.150.35.180	158.245.134.161		
High	6/2/00 1:38:44PM	205.150.35.180	158.245.42.53		
High	6/2/00 1:38:48PM	205.150.35.180	158.245.42.53		
High	6/2/00 1:38:52PM	205.150.35.180	158.245.42.53		
High	6/2/00 5:15:04PM	205.150.35.180	158.245.123.44		
High	6/2/00 5:15:09PM	205.150.35.180	158.245.123.44		
High	6/2/00 5:15:14PM	205.150.35.180	158.245.123.44		
Event:					
IPProtocolViolation					
Priority	Date	From	To	Information	
Medium	6/1/00 7:42:30PM	207.142.81.3	158.236.10.131	REASON 21	Unusual TCP flag combination
Medium	6/1/00 7:42:57PM	207.142.81.3	158.236.10.131	REASON 21	Unusual TCP flag combination
Medium	6/2/00 12:48:56AM	216.10.164.241	192.156.46.98	REASON 6	Unusual TCP flag combination
Medium	6/2/00 12:48:56AM	216.10.164.241	192.156.46.98	REASON 6	Unusual TCP flag combination
Medium	6/2/00 12:48:56AM	216.10.164.241	192.156.46.98	REASON 6	Unusual TCP flag combination
Medium	6/2/00 12:49:02AM	216.10.164.241	192.156.46.98	REASON 6	Unusual TCP flag combination
Event:					
IPUnknownProtocol					
Priority	Date	From	To	Information	

Page 31

Start RealSecure Exploring - Reporting stuff policy Editor.bmp - Paint d:\Program Files\MSS... 7:01 PM



Graph





Raw Logs (RealSecure)

Microsoft Access - [RSLog : Table]											
File Edit View Insert Format Records Tools Window Help											
ID	EventDate	EventName	ProtocolID	SourcePort	DestinationPort	SourcePortName	DestinationPortName	SourceAddress	DestinationAddress	SourceMask	DestinationMask
+	2616888	00 12:48:35 AM SYN Flood	6	0	80 Any	HTTP	0	1759267281	0		
+	2616889	00 1:13:39 AM SYN Flood	6	0	80 Any	HTTP	0	-2111048567	0		
+	2616890	00 1:21:45 AM SYN Flood	6	0	80 Any	HTTP	0	-1395853616	0		
+	2616891	00 1:23:22 AM IP Half Scan	6	64	1521 64	1521	667485708	1928457374	1		
+	2616892	00 2:58:20 AM SYN Flood	6	0	25 Any	E-mail	0	603118018	0		
+	2616893	00 3:31:00 AM SYN Flood	6	0	25 Any	E-mail	0	586340802	0		
+	2616894	00 3:33:30 AM SYN Flood	6	0	25 Any	E-mail	0	250796482	0		
+	2616895	00 3:34:45 AM SYN Flood	6	0	25 Any	E-mail	0	116578754	0		
▶	2616896	00 3:56:53 AM SYN Flood	6	0	1601 Any	1601	0	40660429	0		
+	2616897	00 4:55:10 AM SYN Flood	6	0	80 Any	HTTP	0	682160333	0		
+	2616898	00 5:47:29 AM SYN Flood	6	0	80 Any	HTTP	0	-126934824	0		
+	2616899	00 6:49:52 AM SYN Flood	6	0	80 Any	HTTP	0	438995663	0		
+	2616900	00 7:20:51 AM SYN Flood	6	0	8080 Any	Httpd	0	-101401395	0		
+	2616901	00 7:44:29 AM SYN Flood	6	0	80 Any	HTTP	0	1556029656	0		
+	2616902	00 7:53:46 AM SYN Flood	6	0	80 Any	HTTP	0	-1272680744	0		
+	2616903	00 8:34:27 AM SYN Flood	6	0	80 Any	HTTP	0	232784337	0		
+	2616904	00 8:39:44 AM SYN Flood	6	0	25 Any	E-mail	0	50364360	0		
+	2637923	00 8:56:33 AM SYN Flood	6	0	80 Any	HTTP	0	216007121	0		
+	2637924	00 9:03:04 AM SYN Flood	6	0	80 Any	HTTP	0	199229905	0		
+	2637925	00 9:04:39 AM SYN Flood	6	0	80 Any	HTTP	0	316670417	0		
+	2637926	00 9:05:02 AM SYN Flood	6	0	80 Any	HTTP	0	299893201	0		
+	2637927	00 9:05:02 AM SYN Flood	6	0	80 Any	HTTP	0	266338769	0		
+	2637928	00 9:05:10 AM SYN Flood	6	0	80 Any	HTTP	0	249561553	0		
+	2637929	00 9:05:42 AM SYN Flood	6	0	80 Any	HTTP	0	283115985	0		
+	2637930	00 9:38:26 AM SYN Flood	6	0	80 Any	HTTP	0	1556029656	0		
+	2637931	00 11:33:07 AM SYN Flood	6	0	80 Any	HTTP	0	-141908019	0		
+	2637932	00 12:28:51 PM SYN Flood	6	0	80 Any	HTTP	0	-2011160104	0		
+	2637933	00 12:53:09 PM SYN Flood	6	0	80 Any	HTTP	0	232784337	0		
+	2637934	00 1:04:20 PM SYN Flood	6	0	443 Any	HTTPS	0	133374168	0		
+	2637935	00 1:21:11 PM SYN Flood	6	0	80 Any	HTTP	0	-1912370483	0		
+	2637936	00 1:21:15 PM SYN Flood	6	0	80 Any	HTTP	0	-2014070319	0		
+	2637937	00 1:22:19 PM SYN Flood	6	0	80 Any	HTTP	0	704875213	0		
+	2637938	00 1:23:14 PM SYN Flood	6	0	80 Any	HTTP	0	1711508173	0		
+	2637939	00 1:23:36 PM SYN Flood	6	0	80 Any	HTTP	0	-1241281843	0		
+	2637940	00 1:26:30 PM SYN Flood	6	0	80 Any	HTTP	0	369330893	0		
+	2637941	00 1:27:45 PM SYN Flood	6	0	80 Any	HTTP	0	1375963853	0		

Record: 9 of 128968

0=TCP,1=UDP,2=ICMP, 3=Unknown or ARP.



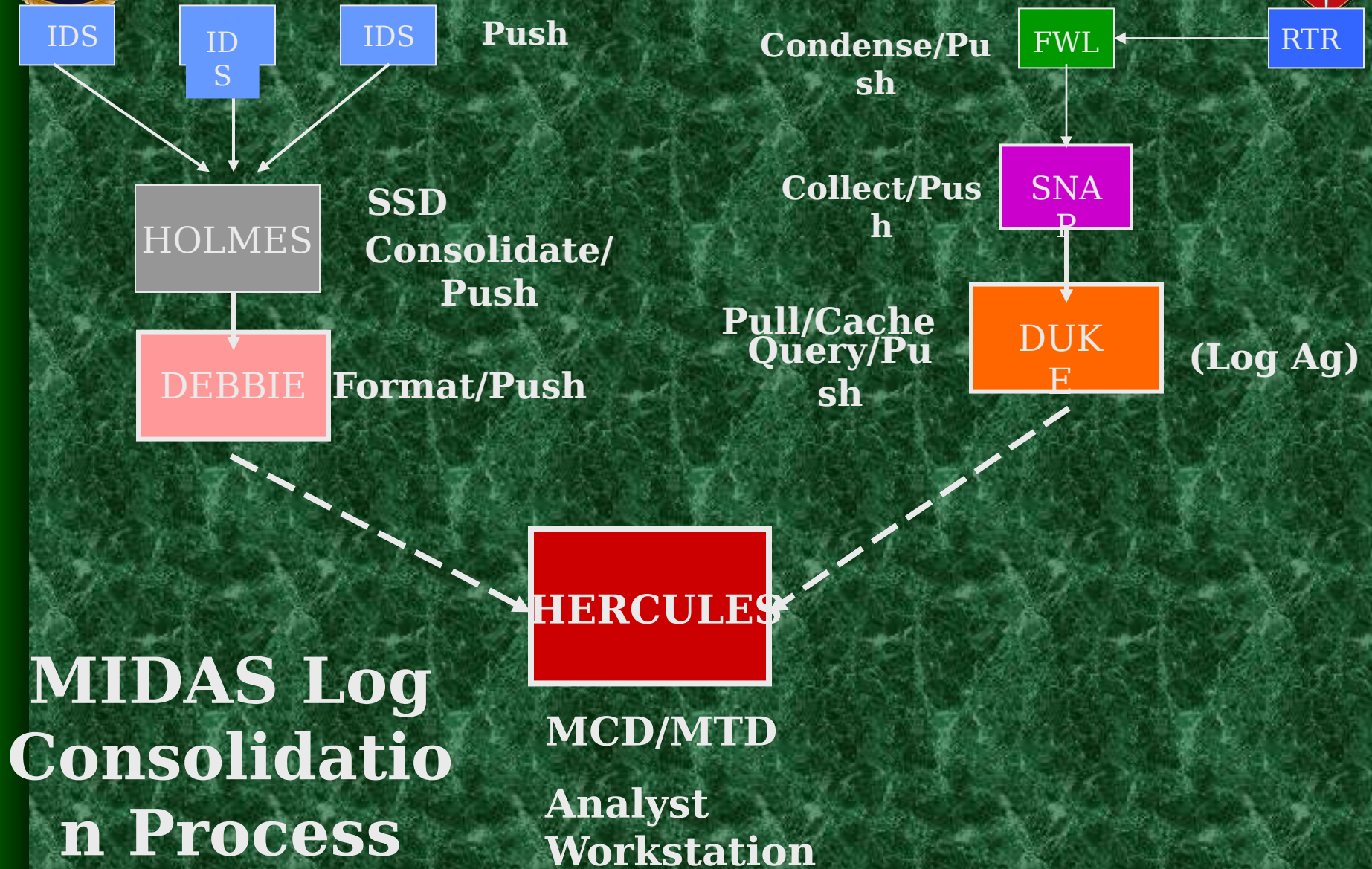
Data Collection and Reporting

Log file Aggregation
JCD - MCD - MTD



Log File Aggregation Tool

- Capabilities
 - Ability to aggregate Firewall, Router and IDS logs
 - Central repository
 - Ability to query on one or more data sets





Joint Cert Database (JCD)

- Needed common database for all to use.
- Managed by JTF-CND
- Operated by DOD-CERT (Technical Arm of JTF-CND)



MIDAS Collection Database (MCD)

- Purpose
 - Maintain a coherent MCEN specific event / incident database
 - Vehicle for reporting MCEN incidents to the DOD-CERT via the Joint CERT Database (JCD)



MCD Capabilities

- Provides 3 levels of authority
 - Console Operator
 - Shift Controller
 - Releasing Authority
- Holds responsible parties to task
- Eliminates over-redundancy
- Easily accessible for viewing



View of MCD Interface

USMC NET INCIDENTS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss

Address http://hercules/niweb/ Go Links »

USMC Net Incidents

Logout Main Menu New Incident View/Edit Incident Pending Incidents Submitted Incidents Help About

Create New Incident

MIDAS# 2000060501 (JCD# 2000-00014)

1. Basic Event Data. Last Updated: (NotModifiedYet) This section to be completed by the Console Operator.

Operator Name	Date Released (YYYYMMDD HH:MM:SS Z) (Not Released Yet)	Status 0 - Open	# Systems Affected <input type="text"/>
Audit Log available? <input type="text"/>	How was the event detected? <input type="text"/>	Noted anomalies? <input type="text"/>	

2. Event Details. Last Updated: (NotModifiedYet) This section to be completed by the Shift Controller.

Shift Controller Name 5 - Mr. Axberg	Date Released (YYYYMMDD HH:MM:SS Z) Not Released Yet	Generation <input type="text"/>
---	---	------------------------------------

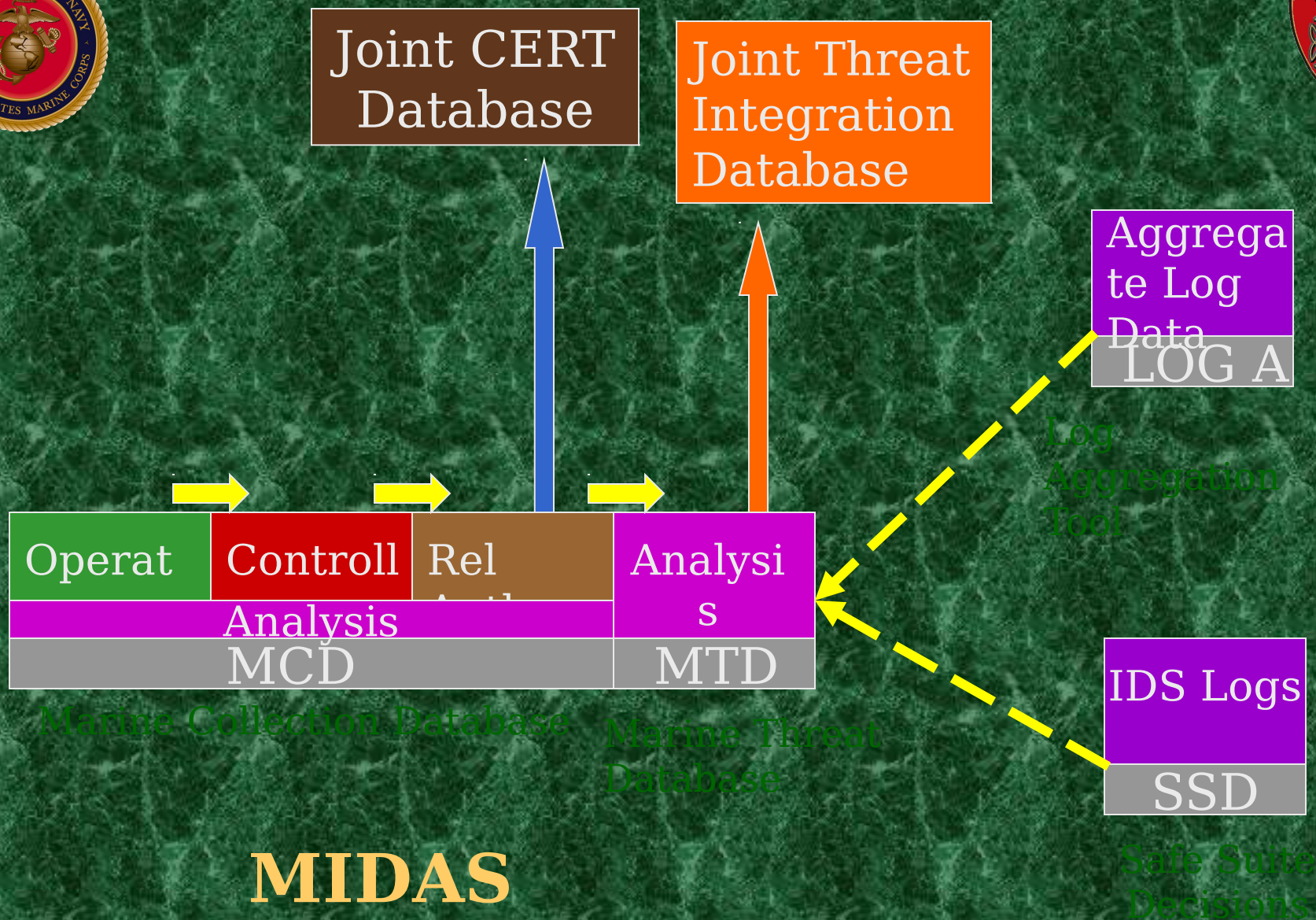
Summary of the event(s)

Actions taken

Residual Damage Noted

Done Local intranet

Start USMC NET INCIDENTS... 6:29 AM



MIDAS

Information Flow



STRATEGIC ANALYSIS

- Analyze All MCEN logs archived
- Key on trends
- Build Profiles
- Prepare and disseminate time-sensitive Evaluations of the scope and immediacy of Cyber Threats posed by individuals and Groups in the U.S. and abroad.
- Manage the Marine Threat Database (MTD)

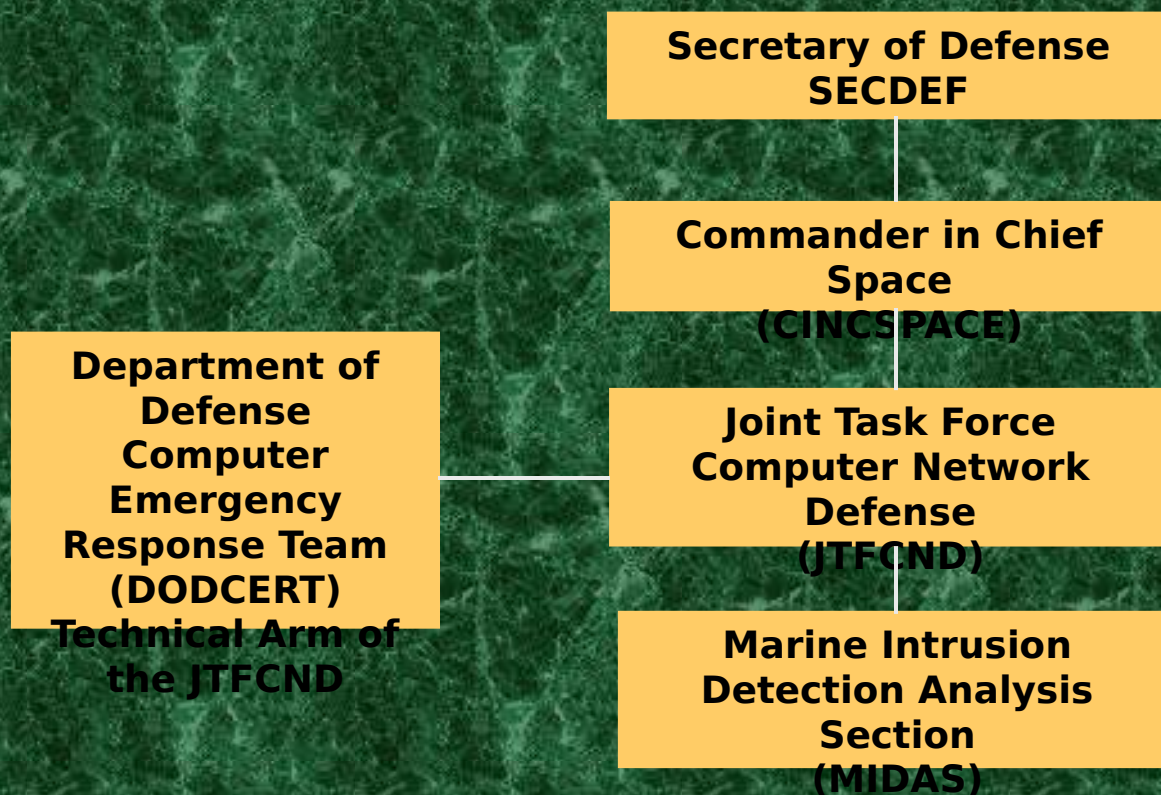


MTD Capabilities

- Maintain profiles on hostile entities
 - Nation States
 - Terrorist cells/groups
 - Hacker(s) and hacker groups
 - Other entities having malicious intent
- Maintain historical data from multiple sources relevant to ongoing analysis
- Ability to infuse immediate threat analysis in order to effect current and future incidents



Incident Reporting Chain of Command





QUESTIONS ?